



TITLE:

Two-Element Generation Of The Hyperbolic
Orthogonal Groups Over The Finite Field
 \mathbb{F}_2 (Semigroups, Formal
Languages and Combinatorics on Words)

AUTHOR(S):

石橋, 宏行

CITATION:

石橋, 宏行. Two-Element Generation Of The Hyperbolic Orthogonal Groups Over The Finite Field
 \mathbb{F}_2 (Semigroups, Formal Languages and Combinatorics on Words). 数理解析研究所講究録 1995, 910: 36-39

ISSUE DATE:

1995-05

URL:

<http://hdl.handle.net/2433/59541>

RIGHT:

Two-Element Generation Of The Hyperbolic Orthogonal Groups Over The Finite Field \mathbb{F}_2

城西大・理 石橋宏行 (Hiroyuki Ishibashi)

位数 2 の素体 $\mathbb{F}_2 = \{0, 1\}$ 上の n 次元双曲型空間 V 上の直交群 $O_n(V)$ の 2 元生成につき考察する。

まず V と $O_n(V)$ の定義及びそれらの基本的性質、主定理、そしてその証明の順に述べる。

\mathbb{F}_2 を K と書く。 V は 2 次写像 (quadratic map) $q: V \rightarrow K$ を付与されている K 上の n 次元ベクトル空間とする。即ち q は

$$q(ax) = a^2 q(x), \quad a \in K, \quad x \in V$$

を満たし、 $B: V \times V \rightarrow K$ を q を用いて、

$$B(x, y) = q(x + y) - q(x) - q(y)$$

により定義すれば B は対称双 1 次形式 (symmetric bilinear form) である。以後簡単のため $B(x, y)$ を xy と書く。 V を K 上の 2 次空間 (quadratic space) と言い、一般線型群 (general linear group) $GL_n(V)$ の部分群

$$O_n(V) = \{\sigma \in GL_n(V) \mid q(x) = q(\sigma x)\}$$

を V 上の直交群 (orthogonal group) と言う。

V の部分集合 U に対し、 $U^\perp = \{x \in V \mid xU = 0\}$ を U の V における直交補と言う。

V の部分空間 U, W に対し、 $V = U \oplus W$ かつ $UW = 0$ のとき $V = U \perp W$ で示し V は U と W の直交和であると言う。

V の任意の元 $x \neq 0$ に対し、 V の元 y で $xy \neq 0$ となるものが存在する時 V を非退化と言う。

V の元 $x \neq 0$ は $q(x) = 0$ の時 isotropic と言い $q(x) \neq 0$ の時 anisotropic と言う。又 V の部分空間 U は isotropic な元を含む時 isotropic 含まない時 anisotropic と言う。

V の 2 元 x, y が $x^2 = y^2 = 0$ かつ $xy = 1$ をみたす時 x, y を双曲対 (hyperbolic pair) と言い x, y を基底 (base) とする 2 次元部分空間 $H = Kx \oplus Ky$ を双曲型平面 (hyperbolic plane) と言う。

体 K の標数が 2 であるから V の任意の元 x に対し、常に $x^2 = 2q(x) = 0$ が成り立つ。従って $xy = 1$ をみたせば x, y は hyperbolic pair である。又、 K の標数が 2 である事から n は偶数となる、そこで $n = 2m$ とおくと V は次のように分解される。

$$V = H_1 \perp H_2 \perp \cdots \perp H_m$$

ここで H_1, H_2, \dots, H_{m-1} は hyperbolic plane であり、 H_m は hypoerbolic か anisotropic である。本講においては H_m が hyperbolic plane、従って、 V が m 個の hyperbolic plane H_1, H_2, \dots, H_m の直交和になる場合、即ち V が双曲型空間 (hyperbolic space) となる場合のみを扱う事にする。

次に各 $H_j, j = 1, 2, \dots, m$ の hyperbolic base $\{x_{2j-1}, x_{2j}\}$ をとり固定する。このとき $X = \{x_1, x_2, \dots, x_{2m-1}, x_{2m}\}$ は V の basis であるが、これを V の hyperbolic base と呼ぶ。

又、簡単のため、 $u = x_1, v = x_2, H = H_1$ とおく。ここで $O_n(V)$ の生成に用いられる特別な元をいくつか定義する。

まず、 $q(x) \neq 0$ なる V の元 x に対し τ_x を

$$\tau_x z = z + zx \cdot x, \quad z \in V.$$

で定義し、又 L の元 x に対し $E(u, x)$ を

$$E(u, x)z = z + zx \cdot u + zu \cdot x + zu \cdot q(x) \cdot u, \quad z \in V.$$

と定義すれば、これらはいずれも $O_n(V)$ の元である。

更に、 $\Delta : u \rightleftharpoons v$ かつ $\Delta = 1$ on L なる V の線型写像はやはり $O_n(V)$ の元であり、従って $E(v, x) = \Delta E(u, x) \Delta$ も $O_n(V)$ の元である。 τ_x を symmetry $E(u, x), E(v, x)$ を Eichler transformation と言う。

次の定理が成り立つ。

定理. $\mathbb{F}_2 = \{0, 1\}$ を位数 2 の素体、 V を \mathbb{F}_2 上の n 次元 hyperbolic space、 $O_n(V)$ を V 上の直交群とすると、 n は偶数であり、 $n = 2m \geq 4$ ならば $O_n(V)$ は位数 4 の元 σ と位数 $2(m-1)$ の元 ρ とにより生成される。

(注意). $O_n(V)$ は V が isotropic ならば S_2 に、anisotropic ならば S_3 と同型になる。従って、 $O_2(V)$ は位数 2 の 1 元又は 2 元で生成される。

定理の証明. L の subset M に対し、 $E(u, M) = \{E(u, x) \mid x \in M\}, E(v, M) = \{E(v, x) \mid x \in M\}$ と定義する。我々は [1, Lemma 2.1] より次が成り立つ事を知っている。

(*) もし $O_n(V)$ の部分群 G が $E(u, L)$ と $E(v, L)$ を含み、更に $O_n^+(V)$ の元 δ を含めば $G = O_n(V)$ である。

ここで $O_n^+(V)$ は Dickson invariant 0 の $O_n(V)$ の元全体から成る指数 2 の部分群である。

さて、そこで $Y = \{x_3, x_4, \dots, x_{2m-1}, x_{2m}\}$ に対し、

$$E_0 = E(u, Y) \cup E(v, Y) \quad \text{の偶数個の元の積の全体}$$

$$E_1 = E(u, Y) \cup E(v, Y) \quad \text{の奇数個の元の積の全体}$$

とおき、

$$E = E_0 \cup E_1$$

とおけば、明らかに、 E_1 の任意の元 γ に対し $E_1 = \gamma E_0$ である。又、 $[1, (2, 5)]$ より $E(u, L) \cup E(v, L) \subseteq E$ であるから (*) より

$$(**) \quad \forall \gamma \in E_1, \forall \delta \notin O_n^+(V) \text{ に対し、} O_n(V) = \langle E_0, \gamma, \delta \rangle$$

を得る。

この事から我々は次の (i), (ii) を満たす δ, ρ を求めればよい事になる。

$$(i) \quad \delta \notin O_n^+(V)$$

$$(ii) \quad \text{ある } \gamma \in E_1 \text{ に対し、} E_0 \cup \{\gamma\} \subseteq \langle \delta, \rho \rangle.$$

ここで $O_n(V)$ の 2 元 Δ', θ を $\Delta' : x_3 \rightleftharpoons x_4$ かつ $\Delta' = 1$ on H_2^\perp 、又 $\theta : x_3 \rightarrow x_5 \rightarrow \dots \rightarrow x_{2m-1} \rightarrow x_3, x_4 \rightarrow x_6 \rightarrow \dots \rightarrow x_{2m} \rightarrow x_4$ かつ $\theta = 1$ on H により定義し、これらに対し δ, ρ を

$$\delta = \Delta E(u, x_3)$$

$$\rho = \begin{cases} \Delta' \theta & (m \text{ が奇数のとき}) \\ \Delta' \theta \Delta & (m \text{ が偶数のとき}) \end{cases}$$

と定義すれば、明らかに $\delta \notin O_n^+(V)$ であるから (i) が成り立つ。従って (ii) を示せばよい。

$G = \langle \Delta, \rho \rangle$ とおくと、 $\delta^3 = \Delta E(v, x_3) \in G$ であるから、 δ と δ^3 を ρ で繰り返して変換すれば、即ち、 $\rho \delta \rho^{-1}, \rho^2 \delta \rho^{-2}, \dots$ 及び $\rho \delta^3 \rho^{-1}, \rho^2 \delta^3 \rho^{-2}, \dots$ を作ると、

$$\Delta E(u, Y) \cup \Delta E(v, Y) \subseteq G$$

を得る。一方 E_0 の任意の元 σ は

$$\sigma = E(w_1, y_1) \cdots E(w_{2r}, y_{2r}) \text{ with } w_i \in \{u, v\} \text{ and } y_i \in Y$$

と表せるから、これを変形すると、

$$\sigma = \Delta E(\Delta w_1, y_1) \Delta E(x_2, y_2) \cdots \Delta E(\Delta w_{2r-1}, y_{2r-1}) \Delta E(w_{2r}, y_{2r}),$$

と成り、 σ は G に含まれる事がわかる。即ち

$$(a) \quad E_0 \subseteq G$$

である。従って G の元 γ で E_1 に含まれるものがある事を示せばよい。まず、

$$\Delta \Delta' = E(u, x_4) E(u, x_3) E(v, x_4) E(v, x_3) E(u, x_4) E(v, x_3)$$

より、

$$(b) \quad \Delta \Delta' \in E_0$$

である。次に、 $1 \leq h < k \leq m$ に対し、 $O_n(V)$ の元 π_{hk} を $x_{2h-1} \rightleftharpoons x_{2k-1}$, $x_{2h} \rightleftharpoons x_{2k}$ かつ $\pi_{hk} = 1$ on $(H_h \perp H_k)^\perp$ と定義すれば、

$$\pi_{hk} = \pi_{1h} \pi_{1k} \pi_{1h},$$

$$\pi_{1r} = E(u, x_{2r}) E(v, x_{2r-1}) E(u, x_{2r}) \text{ for } 1 < r \leq m,$$

$$\theta = \pi_{23} \pi_{34} \cdots \pi_{(m-1)m}.$$

従って、

$$(c) \quad m \text{ が偶数のとき } \theta \in E_0 \text{ であり、} m \text{ が奇数のとき } \theta \in E_1 \text{ である。}$$

を得る。これら (a), (b), (c) から γ の存在を知る事が出来る。実際、もし m が偶数なら

$$\gamma = \delta \rho = \Delta E(u, x_3) \Delta' \theta = \Delta \Delta' \theta E(u, \theta^{-1} \Delta' x_3) \in \mathbb{E}_1 \cap G$$

であり、もし m が奇数なら

$$\gamma = \theta = \Delta \theta \Delta = \Delta \Delta' \rho \in \mathbb{E}_1 \cap G$$

である。故に、 $G = O_n(V)$ 、又 $\text{ord } \delta = 4$ 、 $\text{ord } \rho = 2(m-1)$ であるから、定理の証明は完結する。

References

- [1] H. Ishibashi and A. Earnest, Two-Element Generation of Orthogonal Groups over Finite Fields, J. Algebra 165 (1994), 164-171.